# Calculating the Risk of a Finding

*Proposed Standard Methodology for the Department of Education Audit Resolution Working Group*

**March 17, 2004**

# Plan Overview

- Develop a standard, Department-wide methodology for classifying and calculating the risk of a finding
- Agree on assumptions
- Classify findings by major NIST 800-26 categories (management, operational, and technical), then by subcategories (eg, Physical Security, Production I/O Controls, Logical Access Controls)
- Develop standard risk-calculation methodology
- Calculate the risk for a sample finding

© 2004 BearingPoint, Inc.

# Assumptions

- **NOT a methodology for conducting a full risk assessment**
- **The Department will recognize the three NIST-prescribed FIPS 199 levels of risk for confidentiality, integrity, and availability: high, moderate, and low**
- **System and contract staff will be involved in calculating risk levels—eg, system administrators, database administrators, system owners, system security officers.**

**Detailed system knowledge is critical to correctly calculating risk**

© 2004 BearingPoint, Inc.

# How is Risk Calculated?

- **Impact x Likelihood = Risk**
  - Impact = Sensitivity x Criticality
    - determine whether threat/vulnerability impacts confidentiality, integrity, or availability
    - CIP survey determines the *highest* criticality ranking for the system as a whole; other subsystems could be ranked at a *lower* criticality ranking
  - Likelihood = Threat Capability versus Countermeasure Effectiveness
    - Threat Capability = means, motivation, opportunity, and environment (which subsystem is affected)
  - Risk is ranked as either high, moderate, or low
- Major steps in risk calculation, in order:
  - Determine whether finding is a false positive; if yes, provide justification and *end process here.* If finding is *not* a false positive, go to the step below.
  - Determine whether threat/vulnerability affects confidentiality, integrity, or availability. Determine criticality of affected system or subsystem.
  - Determine Impact—High, Moderate, or Low.
  - Determine Likelihood—High, Moderate, or Low.
  - Determine Risk—High, Moderate, or Low.

© 2004 BearingPoint, Inc.

# Determining Impact

| | System Criticality | | |
|---|---|---|---|
| **Information Sensitivity** | *Mission Critical* | *Mission Important* | *Mission Supportive* |
| *High* | High | High | Moderate |
| *Moderate* | High | Moderate | Moderate |
| *Low* | Moderate | Moderate | Low |

**Impact = Information Sensitivity x System Criticality**

**CIP Survey determines *highest* possible criticality rating for the system as a whole; specific subsystems could be rated *lower* for criticality**

© 2004 BearingPoint, Inc.

# Determining Likelihood (the tough one)

| | **Countermeasure Effectiveness** | | |
|---|---|---|---|
| **Threat Capability** | *High* | *Moderate* | *Low* |
| *High* | Moderate | High | High |
| *Moderate* | Low | Moderate | Moderate |
| *Low* | Low | Low | Low |

**Likelihood = Threat Capability versus Countermeasure Effectiveness**

**Threat Capability = motivation, opportunity, means, and environment (which particular subsystem is affected)**

© 2004 BearingPoint, Inc.

# Putting It All Together: Determining Risk

| | **Likelihood** | | |
|---|---|---|---|
| **Impact** | *High* | *Moderate* | *Low* |
| *High* | High | Moderate * | Low* |
| *Moderate* | Moderate * | Moderate | Low |
| *Low* | Low * | Low | Low |

*** Downgraded from current ED risk assessment policy (Document OCIO-07 )**

© 2004 BearingPoint, Inc.

# Current ED risk assessment policy vs. proposed methodology

- **Proposed methodology has lower risk rankings in four categories compared to current ED risk assessment policy (Document OCIO-07) (NOTE: Proposed methodology meets all NIST 800-30A minimum requirements)**
- **Lower risk rankings are in the following categories:**
  - high impact/moderate likelihood (downgraded from “high” to “moderate”)
  - high impact/low likelihood (from “moderate” to “low”)
  - moderate impact/high likelihood (from “high” to “moderate”)
  - low impact/high likelihood (from “moderate” to “low”)
- **Would ED policy have to be changed to reflect these new rankings?**

© 2004 BearingPoint, Inc.

# Sample Risk Calculation

**Finding: Norton Antivirus is not installed on NT servers**

***To calculate the risk of this finding:***

**Step 1: Identify the system and its system criticality/CIA rankings: For example:**

| **System XYZ** | |
|---|---|
| Confidentiality | High |
| Integrity | High |
| Availability | High |
| Mission critical, important, or supportive? | Mission important |

*continues*

© 2004 BearingPoint, Inc.

# Sample Risk Calculation (continued)

## Step 2: Calculate Impact:

- Which data sensitivity areas does the threat impact: confidentiality, integrity, or availability? (Can be more than one, or all three.)
- Finding affects both integrity and availability—both are rated "high; so information sensitivity is rated "high" (note: in case of different ratings, *always* go with the highest rating).
- Determine mission criticality. System XYX is "mission important."
- So . . . "High Sensitivity" x "Mission Important" = HIGH IMPACT.

## Step 3: Calculate Likelihood:

- Countermeasure effectiveness is rated "low." (System has few controls to mitigate threat.)
- Threat capability is rated "moderate." (Threat-source is motivated and capable, but there are controls in place to mitigate this capability.)
- So . . . "Low Countermeasure Effectiveness" versus "Moderate Capability" = MODERATE LIKELIHOOD

*continues*

© 2004 BearingPoint, Inc.

# Sample Risk Calculation (continued)

**Step 4: Determine Risk:**

**High Impact x Moderate Likelihood =**

**MODERATE RISK**

© 2004 BearingPoint, Inc.